Theorems on groups of substitutions.

By Mr. L. Sylow at Frederikshald in Norway.

It is known that if the order of a group of substitutions is divisible by a prime number n, the group always contains a substitution [=element] of order n. This important theorem is contained in another more general than this: "If the order of a group is divisible by n^α, n being prime, the group contains a partial bundle [=subgroup] of order n^α". The demonstration [=proof] itself of the theorem furnishes some other general properties of groups of substitutions. I append to these some more, less general, propositions which are connected with them or which follow from them, of which several however are already known by a work of Mr. E. Mathieu.

The notation and terms used are those of Mr. C. Jordan.

1. If G is a group of substitutions whose order N is divisible by the prime number n, it is known that G contains a substitution of order n, but we can suppose more generally that it contains a group g of order n^α, in which consequently each substitution is of order a divisor of n^α. We denote the substitutions of g by

$$1, \theta_1, \theta_2, \ldots$$

whereas the substitutions of G in general are denoted by

$$1, \psi_1, \psi_2, \ldots.$$

Finally we shall suppose that G does not contain any partial group [=subgroup] whose order is a power of n greater than n^α. Now G always contains substitutions permutable with [=normalizing] g, to wit the substitutions of the latter themselves, but it is possible that it contains a larger number; in any case these substitutions form a group γ, which contains g, and whose order will be denoted $n^\alpha \nu$; this number is in turn a divisor of N; thus we may set:

$$N = n^\alpha \nu h.$$

The substitutions of the group γ will be denoted by

$$1, \varphi_1, \varphi_2, \ldots.$$

The θ are thus comprised among the φ, just as the latter among the ψ.

That set, we are first going to show that the number ν must be prime to n. Let $x_0, x_1, x_2, \ldots$ be the letters which the group G permutes among themselves, and let y_0 be a rational function of the x, invariant under the substitutions of g but variable under every other function. [In effect, y_0 is a point whose stabilizer is g.] This function [=point] takes, under the substitutions of γ, the ν different values

$$y_0, y_1, y_2, \ldots, y_{\nu-1}.$$

Every one of these functions is invariant under [=fixed by] the substitutions of g but variable under [=moved by] every other substitution. Indeed, if y_1 is obtained from y_0 by the substitution φ_1, y_1 is invariant under the group transformed [=conjugated] from g by φ_1, but variable under every other substitution; but φ_1 being permutable with g, the transformed group is the same as g. Now if one operates on the y by the substitutions of γ, one will have among these quantities [=points] a group γ' necessarily transitive and isomorphic to [=a quotient of] γ. In order to obtain its order we must divide that of γ by the number of substitutions φ which do not alter [=move] any of the y, that is by n^α. Thus the order of γ' is ν. If now ν were divisible by n, γ' would have to contain a substitution of order n; a corresponding substitution φ_1 of γ would have to fulfil the condition

$${\varphi_1}^n = \theta_a.$$

But since φ_1 is permutable with [=normalizes] g, one sees that in this case the substitutions $\theta_q {\varphi_1}^p$ would form a group of order $n^{\alpha+1}$ contained in G. That being contrary to the hypothesis, one concludes that ν is prime to n.

Let us note here that the θ are the only substitutions in γ whose orders are powers of n. Indeed, if φ_1 is a substitution of γ outside g, the substitutions $\theta_q {\varphi_1}^p$ form a group whose order is equal to $n^\alpha m$, m denoting the exponent of the least high power of φ_1 which belongs to g. Now one sees without difficulty that the only powers of φ_1 which belong to g are those whose exponents are multiples of m, whence it follows immediately that m is a divisor of the order of φ_1. Thus if the order of φ_1 were a power of n, one would have $m = n^\beta$, which is impossible, the group of the $\theta_q {\varphi_1}^p$ not being able to be of order $n^{\alpha+\beta}$.

The number h is also not divisible by n. In order to see this, let us imagine a rational function of the x invariant under the substitutions of γ, but variable under every other substitution. Let z_0 be this function, and let us represent by

$$z_0, z_1, z_2, \ldots, z_{h-1}$$

the h values it takes under the substitutions of G. [In effect, G permutes the points $z_0, \ldots, z_{h-1}$ and γ is the stabilizer of z_0.] Let us carry out the subsitutions of g on the z; under this, z_0 does not vary, but every one of the other z takes a number of values which is a divisor of the order of g, that is a power of n. This power cannot be reduced to unity; if for example z_1 were invariant under

g and z_1 were obtained from [=the image of] z_0 by the subsitution ψ_1, z_0 would have to be invariant under the group transformed from g by ${\psi_1}^{-1}$; now, the only group of order n^α contained in γ being g, ${\psi_1}^{-1}$ would have to be permutable with g, which does not happen. Thus if one partitions the functions [=points] $z_1, \ldots, z_{h-1}$ into systems [=orbits], uniting together those which are permuted amongst themselves by the substitutions of g, the number of functions contained in each system will be a power of n. Consequently the number h is of the form $np+1$. Thus the order of g equals the largest power of n which divides the order of G. The results obtained are summarised as follows:

Theorem 1 *If n^α denotes the largest power of the prime number n which divides the order of the group G, this group contains another, g, of order n^α; if moreover $n^\alpha\nu$ denotes the order of the largest group contained in G whose substitutions are permutable with g, the order of G will be of the form $n^\alpha\nu(np+1)$.*

2. Evidently g is not the only group of order n^α contained in G, except only the case $p = 0$. But one could ask if G contains any others than g and its transforms by the substitutions of G. That is what we are going to investigate. Let g' be a group of order n^α contained in G but different from g, and let

$$1, \theta'_1, \theta'_2, \ldots$$

be its substitutions. Let us carry out these substitutions on the functions z, and combine into systems those which are exchanged amongst themselves by this [=orbits under g']. As we have already said, the number of functions contained in each system must be a divisor of n^α; thus one must have an equality of the form

$$np + 1 = n^a + n^b + n^c + \cdots$$

$n^a, n^b, n^c, \ldots$ denoting the number of functions [=points] contained in the various systems [=orbits]. But that requires that at least one of the exponents $a, b, c \ldots$ is zero; in other terms, at least one of the functions z must be invariant under all the substitutions of g'. Let z_k be this function, and suppose that it is obtained from z_0 by the substitution ψ_k. Now z_k is only invariant under the substitutions ${\psi_k}^{-1}\varphi_a\psi_k$; moreover ${\psi_k}^{-1}\varphi_a\psi_k$ is similar to [=has the same cycle type as?] φ_a, and among the φ_a there are only the θ whose orders are powers of n. Thus one must have

$$\theta'_b = {\psi_k}^{-1}\theta_a\psi_k$$

for all the values of b. The group g' is thus the transform of g under ψ_k.

If furthermore one replaces ψ_k by $\varphi_r\psi_k$, one evidently has the same transformed group. On the other hand ψ_k can only be replaced by $\varphi_r\psi_k$. Indeed if one has

$${\psi_l}^{-1}\theta_a\psi_l = {\psi_k}^{-1}\theta_b\psi_k$$

for every value of a, it follows that

$$\psi_k {\psi_l}^{-1} \theta_a \psi_l {\psi_k}^{-1} = \theta_b$$

whence one concludes that

$$\psi_l {\psi_k}^{-1} = \varphi_r$$

or

$$\psi_l = \varphi_r \psi_k.$$

One can thus state this theorem:

Theorem 2 *Everything being as in the preceding theorem, the group G contains precisely $np+1$ distinct groups of order n^α; they are all obtained by transforming an arbitrary one among them by the substitutions of G, every group being given by $n^\alpha \nu$ distinct transformations.*

By analogous reasoning one sees that every group of order n^β contained in G, β being less than α, is the transform of a group contained in g by a substitution in G, and that there are *at least* $n^\alpha \nu$ ways of obtaining it by transformation. Indeed it is possible that there are more, since from the relation

$$\psi_k {\psi_l}^{-1} \theta_a \psi_l {\psi_k}^{-1} = \theta_b$$

one cannot conclude that

$$\psi_l {\psi_k}^{-1} = \varphi_r$$

unless it holds for every value of a.

3. Now we are going to concern ourselves with the group g. Let us form the transformations [=conjugates] of the substitutions $1, \theta_1, \theta_2, \ldots$ by one of them; as by this one only reproduces them in a different order, one has a substitution [=permutation] among the substitutions θ themselves. If one transforms them successively by all the substitutions of g, one has a group of substitutions; indeed, this follows immediately from the identity:

$${\theta_b}^{-1} {\theta_a}^{-1} \theta_r \theta_a \theta_b = (\theta_a \theta_b)^{-1} \theta_r (\theta_a \theta_b).$$

The group among the θ which one obtains in this way is necessarily intransitive, the identity substitution at least being invariant under the transformations; but there are also other invariant substitutions, as we shall see. Indeed, one can combine into systems those substitutions which are exchanged amongst themselves by the transformations; that done, the transformations will produce a transitive group among the substitutions of each system. Now the number of substitutions θ contained in a system is a divisor of the order of the corresponding group; but one sees by a familiar argument that the order of this group is equal to n^α divided by the number of transformations which do not change any of the substitutions of the system being considered. So therefore the number of transformations contained in each system is a power of n. The identity substitution being invariant, one must have an equality of the form

$$n^\alpha = 1 + n^a + n^b + \cdots$$

where $1, n^a, n^b, \ldots$ are the numbers of substitutions in the various systems. That requires that at least $n-1$ of the exponents $a, b, \ldots$ are zero. There are thus in the group g at least n substitutions, including the identity substitution, which are invariant; in other terms, there are in g at least n substitutions exchangeable [=commuting] with all the substitutions of the group.

Now since, two substitutions being exchangeable, their powers are also, there will always be among the substitutions exchangeable with all the others a substitution of order n. Let θ_0 be this substitution, and let y_0 be a rational function of the x, invariant under ${\theta_0}^i$ but variable under every other substitution, and let us represent by

$$y_0, y_1, y_2, \cdots$$

the $n^{\alpha-1}$ values which it takes under the substitutions of g. By carrying out on the y the substitutions of g one will have among these functions a group isomorphic to [=quotient of] g, whose order is evidently $n^{\alpha-1}$. By virtue of what has just been demostrated this group must contain a substitution of order n exchangeable with all the substitutions of the group. Now let θ_1 be a corresponding substitution in g. Applied n times in succession θ_1 must return all the y to their original places, thus

$${\theta_1}^n = {\theta_0}^a.$$

Moreover, if ϑ denotes an arbitrary substitution of g, θ_1 must produce on the y the same substitution as its transform by ϑ, that is, one has

$$\vartheta^{-1}\theta_1\vartheta = {\theta_0}^b\theta_1.$$

The substitutions ${\theta_0}^i{\theta_1}^k$ evidently constitute a group of order n^2. If now one forms a rational function of the x invariant under the ${\theta_0}^i{\theta_1}^k$, but variable under every other substitution, and one argues on this function as we have argued on y_0, one sees that g must contain a substitution θ_2 which fulfils the conditions

$$\begin{aligned} {\theta_2}^n &= {\theta_0}^c{\theta_1}^d \\ \vartheta^{-1}\theta_2\vartheta &= {\theta_0}^e{\theta_1}^t\theta_2 \end{aligned}$$

Continuing thus one proves the following theorem:

Theorem 3 *If the order of a group is n^α, n being prime, an arbitrary substitution ϑ of the group can be expressed by the formula*

$$\vartheta = {\theta_0}^i{\theta_1}^k{\theta_2}^l \cdots {\theta_{\alpha-1}}^r$$

where

$$\begin{array}{rcl} {\theta_0}^n & = & 1 \\ {\theta_1}^n & = & {\theta_0}^a \\ {\theta_2}^n & = & {\theta_0}^b{\theta_1}^c \\ {\theta_3}^n & = & {\theta_0}^d{\theta_1}^e{\theta_2}^f \\ \cdots & & \cdots \end{array}$$

and where one has

$$\begin{array}{rcl} \vartheta^{-1}\theta_0\vartheta & = & \theta_0 \\ \vartheta^{-1}\theta_1\vartheta & = & {\theta_0}^\beta\theta_1 \\ \vartheta^{-1}\theta_2\vartheta & = & {\theta_0}^\gamma{\theta_1}^\delta\theta_2 \\ \vartheta^{-1}\theta_3\vartheta & = & {\theta_0}^\varepsilon{\theta_1}^\zeta{\theta_2}^\eta\theta_3 \end{array}$$

One sees that [the orders of] the composition factors of the group are all equal to n, thus we can state as a corollary the following proposition:

If the order of an algebraic equation is a power of a prime number, the equation is soluble by radicals.

Let us suppose that the group g is transitive and that the number of letters is equal to n^β. In this case the substitution which we have called θ_0 is regular [=semi-regular], that is it moves all the letters, and all its cycles contain the same number of them; for otherwise it evidently would not be exchangeable with all the substitutions of the group. Moreover the group will be imprimitive; indeed the substitutions will replace the letters contained in one cycle of θ_0 by the letters in another cycle. Thus the equation is divided by the solution of an equation of degree $n^{\beta-1}$ into $n^{\beta-1}$ equations of degree n. Evidently the groups of these last equations, as well as that of the auxiliary equation, will only contain substitutions whose orders are powers of n; the equations of degree n will consequently be abelian. Thus:

Theorem 4 *If the degree of an irreducible equation is n^β, n being prime, and the order of its group is also a power of n, an arbitrary root will be determined by a series of β abelian equations of degree n.*

For the case $n = 2$ the last proposition has been proved by Mr. J. Petersen (Om de ligninger, der kunne lóses ved Kvadratrod etc. Kjóbenhavn 1871). [On the equations which can be solved by square roots etc. Copenhagen.]

These results can even be generalized. Indeed, if the order of the group of an equation is equal to $n^\alpha m$, m being less than n, one has, using theorem 1, $p = 0$, $m = \nu$. Consequently all the substitutions in the group are permutable with [=normalize] the partial group [=subgroup] which we have denoted by g. The group is therefore reduced to g, if one adjoins the functions which we have denoted by $y_0, y_1, \ldots$, and which are the roots of an equation whose order and degree are equal to m. Thus if the auxiliary equation is soluble by radicals, the given equation is also. From there it follows as an immediate consequence that:

Theorem 5 *If the order of an algebraic equation is*

$$n^{\alpha} {n_1}^{\alpha_1} {n_2}^{\alpha_2} {n_3}^{\alpha_3} \cdots,$$

$n, n_1, n_2, n_3, \ldots$ *being primes, if moreover one has*

$$\begin{array}{rcl} n & > & {n_1}^{\alpha_1} {n_2}^{\alpha_2} {n_3}^{\alpha_3} \cdots \\ n_1 & > & {n_2}^{\alpha_2} {n_3}^{\alpha_3} \cdots \\ n_2 & > & {n_3}^{\alpha_3} \cdots \end{array}$$

the equation is soluble by radicals.

4. From the preceding one draws also a simple proof of the theorem of Mr. E. Mathieu: *Every transitive group on n^{α} letters, n denoting a prime number, contains a regular substitution of order n.* (See Mr. Liouville's journal 1861.)

Let G be a transitive group of degree $n^{\alpha}m$, and let N be its order. Now N is divisible by $n^{\alpha}m$; therefore let

$$N = n^{\alpha+\beta} m N',$$

N' being supposed prime to n; let moreover G' be the group of order $n^{\beta}N'$ which contains the substitutions of G which do not move x_0. Now G contains a group g of order $n^{\alpha+\beta}$, and the substitutions of the latter which do not move x_0 form a group g', whose order we denote by n^{γ}. Now g' is evidently contained in G', so we have $\gamma \leq \beta$.

But if one denotes by r the number of places which are successively occupied by x_0, when one applies all the substitutions of g, one has, as is known,

$$r n^{\gamma} = n^{\alpha+\beta}$$

thus

$$r \geq n^{\alpha}.$$

The number r is necessarily a power of n; furthermore, what has just been proved for x_0 holds for each of the x. Thus every letter takes under the group g a number of places which is a power of n equal to or greater than n^{α}.

If we now suppse $m = 1$, we see that g must be transitive. That being so, g must contain a regular substitution as we have already said. The theorem is therefore proved.

There is another case where one can equally prove the existence of regular substitutions. Indeed suppose $\alpha = 1$ with $m < n$. Since $n^2 > mn$, one concludes that each letter takes precisely n different places under the substitutions of g. If therefore one combines into one system the letters which are exchanged amongst themselves, one has m systems [=orbits] each of n letters. Now if c is a cycle of a substitution of g, c will represent a circular [=cyclic] substitution of the n

letters in one system. Now if another substitution of g moves the same letters, this deplacement cannot be other than a power of c, for in the contrary case one could derive from the two substitutions a third which would not be of order n. So if θ is a substitution of g, one has

$$\theta = c_1 c_2 \dots c_r$$

c_k denoting a circular substitution among the letters of the k^{th} system. If now $r < m$, the group g must contain a substitution θ_1 which permutes the letters of the $(r+1)^{\text{st}}$ system, and after what has just been said one has

$$\theta_1 = {c_1}^{\delta} {c_2}^{\varepsilon} \dots {c_r}^{\zeta} c_{r+1} c_{r+2} \dots c_s,$$

the numbers $\delta, \varepsilon, \dots, \zeta$ possibly being zero. One deduces from this

$$\theta^p \theta_1 = {c_1}^{p+\delta} {c_2}^{p+\varepsilon} \dots {c_r}^{p+\zeta} c_{r+1} c_{r+2} \dots c_s.$$

Now, since the number of systems is less than n, one can determine p such that none of the numbers $p+\delta, p+\varepsilon, \dots, p+\zeta$ is equal to zero. One thus obtains a substitution having $r+s$ [*sic*: should be s, here and in the next sentence] cycles. If $r+s < m$, one determines in the same way a substitution of g which has more than $r+s$ cycles; continuing thus one ends by finding a regular substitution.

Theorem 6 *A transitive group on nm letters, n being prime, and $m < n$, contains a regular [=semi-regular] substitution of order n.*

By virtue of these two theorems every transitive group on a number of letters less than 12 contains regular substitutions. But already for degree 12 there exist transitive groups which lack them. Thus the substitutions of the group derived from [=generated by]

$$\begin{aligned} \theta_0 &= (x_0 x_1 x_2)(x_3 x_4 x_5)(x_6 x_7 x_8) \\ \theta_1 &= (x_3 x_4 x_5)(x_6 x_8 x_7)(x_9 x_{10} x_{11}) \\ \varphi &= (x_0 x_3 x_6 x_9 x_1 x_4 x_8 x_{11})(x_2 x_5 x_7 x_{10}) \end{aligned}$$

are similar, some to θ_0, the others to powers of φ. Another example is the group derived from θ_0, θ_1 and the following substitutions

$$\begin{gathered} (x_0 x_3 x_1 x_4)(x_2 x_5)(x_6 x_9 x_7 x_{11})(x_8 x_{10}) \\ (x_0 x_7 x_1 x_6)(x_2 x_8)(x_3 x_9 x_4 x_{11})(x_5 x_{10}). \end{gathered}$$

These two groups are of order 72, and characterize equations soluble by radicals.

5. Let us consider now the transitive groups of prime degree. Let n be the degree, N the order of the group. Since N is divisible by n but not divisible by n^2, one has

$$N = n\nu(np+1).$$

Let us suppose the letters arranged in an order such that a circular substitution of the group is expressed by

$$\theta = |\, k \quad k+1 \,|\,;$$

[i.e. $\theta : k \mapsto k+1$;] then the substitutions permutable with the group derived from [=generated by] θ are of the form

$$|\, k \quad ak+b \,|$$

Now $n\nu$ is equal to the order of this last group, so ν is equal to the number of substitutions of the given group which are of the form $|\, k \quad ak \,|$; so ν is a divisor of $n-1$. Thus one has this theorem:

Theorem 7 *The order of a transitive group on a prime number of letters is of the form $n\nu(np+1)$, where n is the degree, $np+1$ the number of essentially different regular substitutions, that is, which are not powers of each other, and where ν is the number of substitutions of the form $|\, k \quad ak \,|$, an arbitrary circular substitution being denoted by $|\, k \quad k+1 \,|$.*

These results are in part known by the researches of Mr. E. Mathieu, who has proved that the number of essentially different circular substitutions is of the form $np+1$, and that there are at least $\frac{N}{n\nu}$ of them, such a number being derivable from the $|\, k \quad k+b \,|$ by transforming them by the substitutions of the group. What is necessary to add to the propositions of Mr. Mathieu to have the above theorem is thus that all the circular substitutions can be derived in the manner described, a point on which Mr. Mathieu seems to have some doubts.

Let us recall here these two propositions equally due to Mr. E. Mathieu:

1. *If $p > 0$, ν cannot be equal to* 1.

2. *If $p > 0$, and n is of the form $4h+3$, ν cannot be equal to* 2.

Being given the order N of a transitive group on n letters, our theorem permits us to determine the number of circular substitutions and the number of substitutions permutable with the group derived from a circular substitution. Indeed ν, being smaller than n, is completely determined by the congruence

$$\frac{N}{n} \equiv \nu \bmod n;$$

and then one has

$$np+1 = \frac{N}{n\nu}.$$

Let us take as an example the group of degree $\frac{q^r-1}{q-1}$, q being a prime number, which one can derive from the linear group with r indices. If r is an odd prime number, it can happen that $\frac{q^r-1}{q-1}$ is a prime number. Set therefore

$$\begin{aligned} n &= \frac{q^r-1}{q-1} \\ N &= \frac{q^r-1}{q-1}(q^r-q)(q^r-q^2)\dots(q^r-q^{r-1}). \end{aligned}$$

Now one sees easily that q is a primitive root of the congruence

$$z^r \equiv 1 \bmod n;$$

consequently one has

$$z^{r-1}+z^{r-2}+\cdots+z+1 \equiv (z-q)(z-q^2)\cdots(z-q^{r-1}).$$

If one now sets

$$z \equiv q^r \equiv 1,$$

one obtains

$$(q^r-q)(q^r-q^2)\cdots(q^r-q^{r-1}) \equiv r$$

that is

$$\frac{N}{n} \equiv r.$$

If therefore one chooses the indices so that a circular substitution is represented by $|\,k \quad k+1\,|$, the group will contain r substitutions of the form $|\,k \quad ak\,|$ to wit the $|\,k \quad q^ik\,|$; the number of essentially different circular substitutions will be $\frac{q^r-q}{r}(q^r-q^2)\cdots(q^r-q^{r-1})$.

The formula $N = n\nu(np+1)$ considerably reduces the number of divisors of the product $2.3.\dots.n$ which can denote the order of a transitive group. If for example one sets $n=7$, ν must be equal to 6 or 3, except for equations soluble by radicals. But if there exists a group of order $7(7p+1)6$, there is also one of order $7(7p+1)3$ containing those substitutions of the first group which are equivalent to an even number of transpositions. In order to obtain the values of $7p+1$ it therefore suffices to examine the case $n=3$; thus $7p+1$ must be a divisor of the number 2.5.4.3, and consequently equal to one of the numbers $1, 2^3, 5.3, 5.3.2^3$, of which the third must be rejected, since there is no group of order 5.3 on 6 letters. For $n=11$ there will only be 15 cases to examine, etc.

Let us examine now the composition of the groups in question. So let G and H be two transitive groups, and let G be contained in H and permutable with its substitutions. Moreover, let $n(np+1)\nu$ be the order of G, and denote by $\theta_0, \theta_1, \dots, \theta_{np}$ its essentially different circular substitutions. Thus G contains the $np+1$ groups of order n: ${\theta_0}^r, {\theta_1}^r, \dots, {\theta_{np}}^r$. If these groups are transformed by an arbitrary circular substitution in H, which will be denoted by θ', they must be reproduced in another order; thus one has a substitution on the $np+1$ groups. But one sees without difficulty that if a group ${\theta_i}^r$ is not invariant under the transformation, it must form part of a cycle of n groups. Thus at least one of the groups is invariant under the transformation. If we suppose that it is ${\theta_0}^r$, this group is permutable with θ', whence one concludes

$$\theta' = {\theta_0}^b.$$

Indeed, if one chooses the indices such that

$$\theta_0 = |\, k \quad k+1 \,|,$$

there are among the $n(n-1)$ substitutions $|\, k \quad ak+b \,|$, alone permutable with ${\theta_0}^r$, only the $|\, k \quad k+b \,|$ which are of order n. All the circular substitutions in H therefore form part of G.

Conversely, if G and H contain the same circular substitutions, and if H contains G, H is composed with G [i.e. G is a normal subgroup of H]. Always let $n(np+1)\nu$ be the order of G, that of H will be $n(np+1)\nu\nu_1$, ν_1 being a divisor of $\frac{n-1}{\nu}$. The substitutions of the form $|\, k \quad ak \,|$ contained in H are powers of a single one of them; denote the latter by φ; those which belong to G will consequently be the powers of φ^{ν_1}. Now it is easy to see that H derives from [=is generated by] the substitutions $\theta_0, \theta_1, \dots, \theta_{np}, \varphi$. Indeed the group derived from these substitutions is contained in H; on the other hand its order cannot be less than $n(np+1)\nu\nu_1$, since there are $np+1$ circular substitutions and $\nu\nu_1$ substitutions $|\, k \quad ak \,|$. Likewise G is derived from the substitutions $\theta_0, \theta_1, \dots, \theta_{np}, \varphi^{\nu_1}$. Thus G is permutable with the substitutions of H, if it is permutable with φ. Now the latter holds, for firstly the transforms of $\theta_0, \theta_1, \dots, \theta_{np}$ by φ are circular substitutions belonging to H and therefore to G; secondly φ^{ν_1} is exchangeable with φ.

Thus we have proved the following theorem:

Theorem 8 *For a transitive group of prime degree to be composed with a partial group, it is necessary and sufficient that the second group contains all of the circular substitutions of the first.*

Let an equation be given whose group is H. If one forms a function of the roots invariant under the substitutions of G, but variable under every other substitution, it will evidently be a root of an abelian equation of degree ν_1. By adjoining this function one reduces the group of the equation to G.

So if an irreducible equation of degree n is composite, it becomes simple by the adjunction of the root of an abelian equation, whose degree is a divisor of $n-1$.

By supposing $p=0$, one recovers a known property of equations soluble by radicals.